PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-137686
(43)Date of publication of application : 31.05.1996

(51)Int.CI. G06F 9/06
G06F 12/14

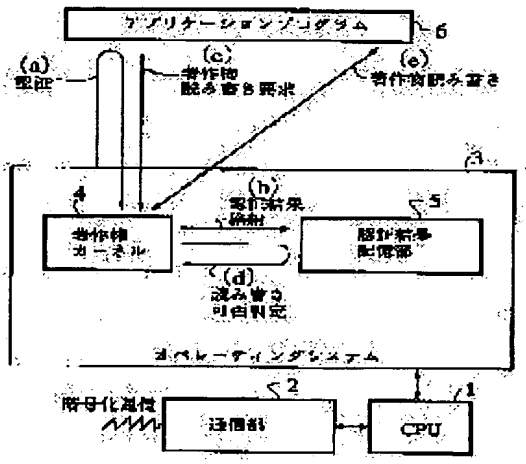
(21)Application number : 07-237489
(22)Date of filing : 14.09.1995

(71)Applicant : TOSHIBA CORP
(72)Inventor : YOSHIDA HIDEKI
IMAI TORU
SEGAWA HIDEO

(30)Priority
Priority number : 06221238 Priority date : 16.09.1994 Priority country : JP

(54) METHOD AND DEVICE FOR MANAGING DATA ON LITERARY WORK

(57)Abstract:
PURPOSE: To prevent violation of copyright by verifying an application program and permitting an access request of the application program when the application program is verified when an access request is made from the application program to literary work data.
CONSTITUTION: A copyright kernel 4 in an operating system(OS) 3 executed by a CPU 1 verifies an application program 6 to discriminate whether or not the application program is a registered program. As a result of verification, when the application program is discriminated to be a program managing correctly a copyright label, it is stored in a storage section 5 in the OS. Then the usual application processing is executed and when the application program 6 makes a read/write request of literary work data to the OS, the OS 3 checks the storage section 5 and accepts the request when it is confirmed that the application program 6 manages the copyright label correct or rejects the request when not.



LEGAL STATUS

[Date of request for examination] 19.09.2000
[Date of sending the examiner's decision of rejection] 09.03.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

JP-A 8-137686

[0048]

(First Embodiment)

In the present embodiment, schematically, a copyright kernel and an authentication result storing mechanism are provided within the OS for performing authentication of the application program upon use of digital signatures.

[0051]

Thereafter, ordinary application processes are performed (S53 in Fig. 2), and in the event a read/write request of copyright data has been issued from the application program 6 to the OS (S54 in Fig. 2, c in Fig. 3), the OS 3 checks up in the above authentication result storing portion 5 (S55 in Fig. 2, d in Fig. 3), and when it is confirmed that the application program 6 properly manages the copyright label (a copyright-compliant application program), the request is accepted (S56 in Fig. 2, e in Fig. 3) but otherwise, rejects the request. With this arrangement, it is possible to perform proper copyright management.

<FIG. 2>

S51: Authenticate application

S52: Store authentication result

S53: Process application

S54: Request read/write of copyright

S55: Read/right availability judged?

S56: Read/write copyright

<FIG. 3>

① 6: Application program

②(a): Authentication

③(c) Request read/write of copyright

④(e): Read/write copyright

⑤ 4: Copyright kernel

⑥(b): Store authentication result

⑦ 5: Authentication result storing portion

⑧(d): Judge read/write availability

⑨ Operating System

⑩ Encoded communication

⑪ Communication portion

Ref. 1

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－137686

(43)公開日　平成８年(1996)５月31日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　9/06	５５０　Ｇ	7230－5Ｂ		
12/14	３１０　Ａ			

審査請求　未請求　請求項の数14　ＯＬ　（全 18 頁）

(21)出願番号　特願平7－237489

(22)出願日　平成７年(1995)９月14日

(31)優先権主張番号　特願平6－221238

(32)優先日　平６(1994)９月16日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　吉田　英樹
神奈川県川崎市幸区小向東芝町１　株式会社東芝研究開発センター内

(72)発明者　今井　徹
神奈川県川崎市幸区小向東芝町１　株式会社東芝研究開発センター内

(72)発明者　瀬川　英生
神奈川県川崎市幸区小向東芝町１　株式会社東芝研究開発センター内

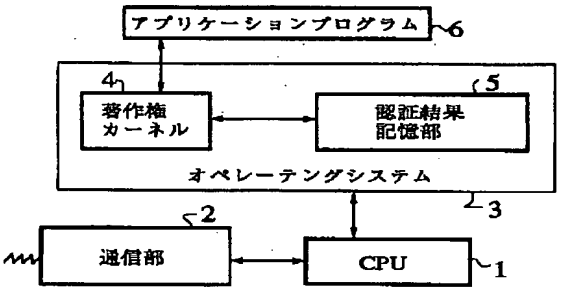
(74)代理人　弁理士　三好　秀和　（外３名）

(54)【発明の名称】　著作物データ管理方法及び著作物データ管理装置

(57)【要約】

【課題】　登録された正当なアプリケーションプログラムのみが絵画・小説などの受動的なデータである著作物を操作できるようにした著作物データ管理方法を提供すること。

【解決手段】　本発明は、マイクロプロセッサ上にて起動中の管理プログラムが、起動されたアプリケーションプログラムと所定の情報の受渡しを行うことによって、該アプリケーションプログラムの認証を行い、管理プログラムは、この認証の結果と、認証した前記アプリケーションプログラムを特定する情報とを組にして認証結果記憶手段に格納し、１つのアプリケーションプログラムから所望の著作物データへのアクセス要求が与えられた場合、管理プログラムは、認証結果記憶手段を参照し、該１つのアプリケーションプログラムが既に認証に成功したものであることが判明したときのみ該アクセス要求を許可することを特徴とする。



1

【特許請求の範囲】

【請求項１】　アプリケーションプログラムを認証する認証手段と、

該認証手段により得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶する記憶手段と、

前記アプリケーションプログラムからの著作物データへのアクセス要求を受け、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証手段による認証の成功を示す時に要求された著作物データへのアクセスを許可する管理手段と、

を有することを特徴とする著作物データ管理装置。

【請求項２】　前記アプリケーションプログラムは所定の暗号鍵で暗号化されており、前記認証手段は前記アプリケーションプログラムを前記所定の暗号鍵に対応する復号鍵で復号化することにより認証することを特徴とする請求項１記載の著作物データ管理装置。

【請求項３】　著作物データに対するアクセスが許可されるべき各著作権遵守アプリケーションプログラムについて、正しいパスワードを記憶するパスワード記憶手段を更に有し、

前記認証手段は前記アプリケーションプログラムのパスワードを前記パスワード記憶手段に記憶された正しいパスワードと照合することにより前記アプリケーションプログラムを認証することを特徴とする請求項１記載の著作物データ管理装置。

【請求項４】　著作物データに対するアクセスが許可されるべき著作権遵守アプリケーションプログラムについて、複数のパスワードとそれらに対応する正しい応答を記憶するパスワード記憶手段を更に有し、

前記認証手段は前記アプリケーションプログラムに前記複数のパスワードの一つを通知し、前記アプリケーションプログラムから受けた応答を前記パスワード記憶手段に記憶された前記複数のパスワードの一つに対応する正しい応答と照合することにより前記アプリケーションプログラムを認証することを特徴とする請求項１記載の著作物データ管理装置。

【請求項５】　前記アプリケーションプログラムは第一のハードウェア内の第一のプロセッサ上で実行され、前記認証手段と前記記憶手段は第二のハードウェア内の第二プロセッサ上で動作し、前記管理手段は前記第一のハードウェア内の第一のプロセッサ上で動作し、前記第一のハードウェアと第二のハードウェアは互いに物理的に分離しており、前記第一のプロセッサと第二のプロセッサは互いに接続されていることを特徴とする請求項１記載の著作物データ管理装置。

【請求項６】　前記認証手段は前記管理手段を含んだオペレーティングシステムが前記第一のプロセッサ上で起動された時に、該オペレーティングシステムも認証することを特徴とする請求項５記載の著作物データ管理装

2

置。

【請求項７】　前記アプリケーションプログラムからのコールに応じて、著作物データの著作権ラベルに対する読み書き動作を行う著作物ラベル読み書きプログラムを更に有することを特徴とする請求項１記載の著作物データ管理装置。

【請求項８】　前記管理手段は、要求されたアクセスが著作物データの読み出しである時には、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証手段による認証の成功を示さない時にも要求された著作物データへのアクセスを許可することを特徴とする請求項１記載の著作物データ管理装置。

【請求項９】　前記管理手段は、どの著作物データがどのアプリケーションプログラムからアクセス可能であるか示す情報を記憶し、前記管理手段は前記記憶手段に記憶された該情報に基づいて前記アプリケーションプログラムからの著作物データへのアクセス要求を許可することを特徴とする請求項１記載の著作物データ管理装置。

【請求項１０】　前記認証手段は前記アプリケーションプログラムが起動された時に認証することを特徴とする請求項１記載の著作物データ管理装置。

【請求項１１】　前記認証手段は前記アプリケーションプログラムが著作物データへのアクセス要求を発した時に認証することを特徴とする請求項１記載の著作物データ管理装置。

【請求項１２】　アプリケーションプログラムを認証する認証手段と、

該認証手段により得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶する記憶手段と、

前記アプリケーションプログラムから発行されるデータ入出力要求を、前記アプリケーションプログラムの識別子と共に受取る要求受理手段と、

前記要求受理手段で受取ったデータ入出力要求がデータ入力要求である時に要求されたデータを前記アプリケーションプログラムに入力するデータ入力手段と、

前記データ入力手段により入力されたデータが保護データであるかどうか判別する保護データ判別手段と、

前記保護データ判別手段が前記データ入力手段により入力されたデータを保護データであると判別した時に、少なくとも前記アプリケーションプログラムの識別子を記録する保護データ入力記憶手段と、

前記要求受理手段で受取ったデータ入出力要求がデータ出力要求である時に、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証手段による認証の成功を示す場合及び前記アプリケーションプログラムの識別子が前記保護データ入力記憶手段に記録されていない場合にデータ出力を許可し、前記アプリケーションプログラムの識別子が前記保護データ入力記録手段に記録されている時にデータ出力を許可するか

どうかを少なくとも要求された出力先に基づいて判定する出力許可判定手段と、
前記出力許可判定手段がデータ出力を許可した時に要求されたデータを出力するデータ出力手段と、
を有することを特徴とする著作物データ管理装置。
【請求項１３】　アプリケーションプログラムを認証するステップと、該認証するステップにより得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶手段に記憶するステップと、
前記アプリケーションプログラムからの著作物データへのアクセス要求を受け、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証するステップによる認証の成功を示す時に要求された著作物データへのアクセスを許可するステップと、
を有することを特徴とする著作物データ管理方法。
【請求項１４】　コンピュータに著作物データの管理を行わせるようにするためのコンピュータにより解読可能なコンピュータプログラムコード手段を実装したコンピュータで利用可能な媒体を有するコンピュータプログラム製品であって、該コンピュータプログラム手段が、
コンピュータによって、アプリケーションプログラムを認証するようにする第一のコンピュータプログラムコード手段と、
コンピュータによって、該第一のコンピュータプログラムコード手段により得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶するようにする第二のコンピュータプログラムコード手段と、
コンピュータによって、前記アプリケーションプログラムからの著作物データへのアクセス要求を受け、前記第二のコンピュータプログラムコード手段により記憶されている前記アプリケーションプログラムの認証結果が前記第一のコンピュータプログラムコード手段による認証の成功を示す時に要求された著作物データへのアクセスを許可するようにする第三のコンピュータプログラムコード手段とを有することを特徴とするコンピュータプログラム製品。
【発明の詳細な説明】
【０００１】
【発明の属する技術】本発明は、計算機システム上で扱われる著作物データの管理を行う著作物データ管理方法および著作物データ管理装置に関する。
【０００２】
【従来の技術】従来、計算機システム上にはセキュリティ機構があり、システム管理者が設定した権限にしたがってファイルなどのデータ管理が行なわれていた。計算機システムを所有する特定の組織および個人が閲覧・変更・配布などの操作を行なう権利を持つデータについては、このような管理が適切である。

【０００３】ところが、プログラム・絵画・小説などの著作物を計算機システム上で扱う場合、システムを所有する組織および個人がその著作物の操作を行なう権利を持っていない場合が多い。具体的には、閲覧や利用はできても、変更や再配布が著作者によって認められていない場合などがある。
【０００４】このような著作物を通常の計算機システムで扱う場合、悪意のシステム管理者がデータのアクセス権限を書き換えたり、システム管理者の権限でデータを読み書きすることによって、著作物を不当に利用されたりする危険がある。
【０００５】このような不都合を回避するため、プログラムの利用の可否をシステム管理者にも侵害できないような方法で管理する「超流通」という概念が提唱されている（森亮一、田代秀一「ソフトウェア・サービス・システム（SSS)の提案」電子情報通信学会論文誌　'87/1 Vol.J70-D No.1 参照）。超流通システムでは、著作物に著作者・利用／配布条件・課金方法などを示すラベル（著作権ラベル）がついており、そのラベルは通常のソフトウェアでは変更することができない。これによって、アプリケーションプログラムの著作権保護を行なうことはできる。
【０００６】これとは別に、米国防総省のＯＳ（オペレーティングシステム）のセキュリティレベル分類（Department of Defense Trusted Computer System Evaluation Criteria, Department of Defense Standard DOD 5200.28-STD,Library Number S225,711, December 1985, 通称 Orange Book）でセキュリティレベルＢに分類されるようなＯＳでは、強制保護という機構を用いることによって、あるデータを読み書きすることを許されているプログラムまたはユーザが、そのデータを、そのデータを読み書きすることを許されていないプログラムまたはユーザに渡すことができないようにすることができる。この方法を著作物に応用することによって、プログラムコードを持たないデータを含めたファイルの保護を行なうこともできる。
【０００７】しかしながら、上記のような従来の著作管理機構では著作権保護を行なう対象はプログラムのみであり、絵画・小説などプログラムコードを持たずに他のプログラムに読み込まれて利用される受動的なデータである著作物を保護する機構は提供されていない。
【０００８】例えば、受動的な著作物に著作権ラベルをつけて保護しようとしても、著作物を読んだ悪意のアプリケーションプログラムが著作権ラベルを不正に管理することが可能である。著作権ラベルの不正な管理方法としては、著作権ラベルを改ざんまたは除去して著作物をコピーするという可能性が挙げられる。
【０００９】また、一部の著作物は、他の著作物を中に含むような形で作成されている場合がある。たとえば、あるテーマに基づいて複数の絵画の画像を編集して画集

を作るといった場合、画集（二次著作物）の著作権のほかに、元の個々の絵画（一次著作物）の著作権をも管理する必要がある。従って、複数の絵画データを編集して画集を作成する機能を持つアプリケーションプログラムでは、一次著作物につけられた著作権ラベルの中の著作者・利用／配布条件・課金方法などを損なわないような著作権ラベルを二次著作物に付加しなければならない。具体的には、著作者として一次著作物の著作者をすべて含め、すべての著作者の利用／配布条件で許されているような利用／配布方法のみを許すほか、すべての著作者にそれぞれ課金が行なわれるような著作権ラベルをつけるといった機構が必要である。

【００１０】ところが、従来の著作管理機構では、アプリケーションプログラムがこのように著作権ラベルを管理することが保証されない。そのため、従来の機構で著作物を保護しようとすると、例えば著作権をアプリケーションプログラムの中にあらかじめ埋め込んでおく必要がある。しかしながら、この方式には、処理の自由度や処理速度が低下する問題がある。さらに、データを読み込んで操作するように書かれた既存のアプリケーションプログラムを修正して著作権管理を行なうように利用することは困難であり、新たにアプリケーションプログラムを開発する必要があるという不具合がある。

【００１１】従来の著作物を保護する方法としては、上記のほかに、著作物を直接アプリケーションプログラムに読み込ませず、毎回ＯＳを経由して著作物に対する操作を行なわせるという方法がある。しかしながら、この方法では、ＯＳが対応した処理しか行なえないため、アプリケーションプログラムに特有な処理を行なうことができないほか、処理のたびにＯＳが呼び出されるために実行時間がかかるという問題がある。

【００１２】一方、従来のセキュリティレベルＢのＯＳでは、アプリケーションプログラムにあるデータが渡されると、そのアプリケーションプログラムがそのデータを読んだ以降にデータを書き込むファイルすべてに、そのデータに基づいて作られたデータが書き込まれる可能性がある、という前提でＯＳによる管理が行なわれる。

【００１３】このようなＯＳを使って著作物管理を行なうと、複数の著作物を次々に読み書きしたりするようなアプリケーションプログラムでは、それまでに一度でも読み込んだ著作物の著作権ラベルが、それ以降に書き込まれた著作物ファイルすべてに付加されるため、本来無関係な著作権ラベルが著作物につけられてしまう場合がある、という問題点がある。

【００１４】

【発明が解決しようとする課題】従来の著作物に著作権ラベルを付加するような著作管理機構では著作権保護を行なう対象はプログラムのみであり、絵画・小説などプログラムコードを持たずに他のプログラムに読み込まれて利用される受動的なデータである著作物を保護する機構は提供されていなかった。

【００１５】また、従来のＯＳを使って著作物管理を行なうような著作管理機構では、絵画・小説などの受動的なデータである著作物に対するアクセスを伴う処理のたびにＯＳが呼び出されるため、処理の実行に時間がかかるという問題点、あるいは著作権ラベルのきめ細かい管理ができず、それまでに一度でも読み込んだ著作物の著作権ラベルが、それ以降に書き込まれた著作物ファイルすべてに付加される問題点などがあった。

【００１６】本発明は、上記事情を考慮してなされたものであり、絵画・小説などプログラム以外の受動的なデータである著作物に対しても、著作権ラベルの管理を正しく行なうものとして登録されたアプリケーションプログラムのみが操作できるような管理のできる著作物データ管理方法及び著作物データ管理装置を提供することを目的とする。

【００１７】

【課題を解決するための手段】本発明は、アプリケーションプログラムを認証する認証手段と、該認証手段により得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶する記憶手段と、前記アプリケーションプログラムからの著作物データへのアクセス要求を受け、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証手段による認証の成功を示す時に要求された著作物データへのアクセスを許可する管理手段と、を有する著作物データ管理装置を提供する。

【００１８】又、本発明は、前記アプリケーションプログラムは所定の暗号鍵で暗号化されており、前記認証手段は前記アプリケーションプログラムを前記所定の暗号鍵に対応する復号鍵で復号化することにより認証することを特徴とする。

【００１９】又、本発明は、著作物データに対するアクセスが許可されるべき各著作権遵守アプリケーションプログラムについて、正しいパスワードを記憶するパスワード記憶手段を更に有し、前記認証手段は前記アプリケーションプログラムのパスワードを前記パスワード記憶手段に記憶された正しいパスワードと照合することにより前記アプリケーションプログラムを認証することを特徴とする。

【００２０】又、本発明は、著作物データに対するアクセスが許可されるべき著作権遵守アプリケーションプログラムについて、複数のパスワードとそれらに対応する正しい応答を記憶するパスワード記憶手段を更に有し、前記認証手段は前記アプリケーションプログラムに前記複数のパスワードの一つを通知し、前記アプリケーションプログラムから受けた応答を前記パスワード記憶手段に記憶された前記複数のパスワードの一つに対応する正しい応答と照合することにより前記アプリケーションプログラムを認証することを特徴とする。

【００２１】又、本発明は、前記アプリケーションプログラムは第一のハードウェア内の第一のプロセッサ上で実行され、前記認証手段と前記記憶手段は第二のハードウェア内の第二プロセッサ上で動作し、前記管理手段は前記第一のハードウェア内の第一のプロセッサ上で動作し、前記第一のハードウェアと第二のハードウェアは互いに物理的に分離しており、前記第一のプロセッサと第二のプロセッサは互いに接続されていることを特徴とする。

【００２２】又、本発明は、前記認証手段は前記管理手段を含んだオペレーティングシステムが前記第一のプロセッサ上で起動された時に、該オペレーティングシステムも認証することを特徴とする。

【００２３】又、本発明は、前記アプリケーションプログラムからのコールに応じて、著作物データの著作権ラベルに対する読み書き動作を行う著作物ラベル読み書きプログラムを更に有することを特徴とする。

【００２４】又、本発明は、前記管理手段は、要求されたアクセスが著作物データの読み出しである時には、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証手段による認証の成功を示さない時にも要求された著作物データへのアクセスを許可することを特徴とする。

【００２５】又、本発明は、前記管理手段は、どの著作物データがどのアプリケーションプログラムからアクセス可能であるか示す情報を記憶し、前記管理手段は前記記憶手段に記憶された該情報に基づいて前記アプリケーションプログラムからの著作物データへのアクセス要求を許可することを特徴とする。

【００２６】又、本発明は、前記認証手段は前記アプリケーションプログラムが起動された時に認証することを特徴とする。

【００２７】又、本発明は、前記認証手段は前記アプリケーションプログラムが著作物データへのアクセス要求を発した時に認証することを特徴とする。

【００２８】更に、本発明は、アプリケーションプログラムを認証する認証手段と、該認証手段により得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶する記憶手段と、前記アプリケーションプログラムから発行されるデータ入出力要求を、前記アプリケーションプログラムの識別子と共に受取る要求受理手段と、前記要求受理手段で受取ったデータ入出力要求がデータ入力要求である時に要求されたデータを前記アプリケーションプログラムに入力するデータ入力手段と、前記データ入力手段により入力されたデータが保護データであるかどうか判別する保護データ判別手段と、前記保護データ判別手段が前記データ入力手段により入力されたデータを保護データであると判別した時に、少なくとも前記アプリケーションプログラムの識別子を記録する保護データ入力記憶手段と、前記要求受理手段で受取ったデータ入出力要求がデータ出力要求である時に、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証手段による認証の成功を示す場合及び前記アプリケーションプログラムの識別子が前記保護データ入力記憶手段に記録されていない場合にデータ出力を許可し、前記アプリケーションプログラムの識別子が前記保護データ入力記録手段に記録されている時にデータ出力を許可するかどうかを少なくとも要求された出力先に基づいて判定する出力許可判定手段と、前記出力許可判定手段がデータ出力を許可した時に要求されたデータを出力するデータ出力手段と、を有する著作物データ管理装置を提供する。

【００２９】更に、本発明は、アプリケーションプログラムを認証するステップと、該認証するステップにより得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶手段に記憶するステップと、前記アプリケーションプログラムからの著作物データへのアクセス要求を受け、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証するステップによる認証の成功を示す時に要求された著作物データへのアクセスを許可するステップと、を有する著作物データ管理方法を提供する。

【００３０】又、本発明は、前記アプリケーションプログラムは所定の暗号鍵で暗号化されており、前記認証するステップは前記アプリケーションプログラムを前記所定の暗号鍵に対応する復号鍵で復号化することにより認証することを特徴とする。

【００３１】又、本発明は、著作物データに対するアクセスが許可されるべき各著作権遵守アプリケーションプログラムについて、正しいパスワードをパスワード記憶手段に記憶するステップを更に有し、前記認証するステップは前記アプリケーションプログラムのパスワードを前記パスワード記憶手段に記憶された正しいパスワードと照合することにより前記アプリケーションプログラムを認証することを特徴とする。

【００３２】又、本発明は、著作物データに対するアクセスが許可されるべき著作権遵守アプリケーションプログラムについて、複数のパスワードとそれらに対応する正しい応答をパスワード記憶手段に記憶するステップを更に有し、前記認証するステップは前記アプリケーションプログラムに前記複数のパスワードの一つを通知し、前記アプリケーションプログラムから受けた応答を前記パスワード記憶手段に記憶された前記複数のパスワードの一つに対応する正しい応答と照合することにより前記アプリケーションプログラムを認証することを特徴とする。

【００３３】又、本発明は、前記アプリケーションプログラムは第一のハードウェア内の第一のプロセッサ上で

実行され、前記認証するステップと前記記憶するステップは第二のハードウェア内の第二プロセッサ上で行われ、前記許可するステップは前記第一のハードウェア内の第一のプロセッサ上で行われ、前記第一のハードウェアと第二のハードウェアは互いに物理的に分離しており、前記第一のプロセッサと第二のプロセッサは互いに接続されていることを特徴とする。

【００３４】又、本発明は、前記認証するステップは前記許可するステップを行うオペレーティングシステムが前記第一のプログラム上で起動された時に、該オペレーティングシステムも認証することを特徴とする。

【００３５】又、本発明は、前記アプリケーションプログラムから著作物ラベル読み書きプログラムをコールするステップと、著作物データの著作権ラベルに対する読み書き動作を前記著作権ラベル読み書きプログラムにより行うステップと、を更に有することを特徴とする。

【００３６】又、本発明は、前記許可するステップは、要求されたアクセスが著作物データの読み出しである時には、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記するステップによる認証の成功を示さない時にも要求された著作物データへのアクセスを許可することを特徴とする。

【００３７】又、本発明は、前記記憶手段は、どの著作物データがどのアプリケーションプログラムからアクセス可能であるかを示す情報を記憶し、前記許可するステップは前記記憶手段に記憶された該情報に基づいて前記アプリケーションプログラムからの著作物データへのアクセス要求を許可することを特徴とする。

【００３８】又、本発明は、前記認証するステップは前記アプリケーションプログラムが起動された時に認証することを特徴とする。

【００３９】又、本発明は、前記認証するステップは前記アプリケーションプログラムが著作物データへのアクセス要求を発した時に認証することを特徴とする。

【００４０】更に、本発明は、アプリケーションプログラムを認証するステップと、該認証するステップにより得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶手段に記憶するステップと、前記アプリケーションプログラムに保護データが入力された時に、少なくとも前記アプリケーションプログラムの識別子を保護データ入力記録手段に記録するステップと、前記アプリケーションプログラムからのデータ出力要求に対し、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証するステップによる認証の成功を示す場合及び前記アプリケーションプログラムの識別子が前記保護データ入力記録手段に記録されていない時にデータ出力を許可し、前記アプリケーションプログラムの識別子が前記保護データ入力記録手段に記録されている時にデータ出力を許可するかどうかを少なくとも要求された出力先に基づいて判定するステップと、を有する著作物データ管理方法を提供する。

【００４１】更に、本発明は、コンピュータに著作物データの管理を行わせるようにするためのコンピュータにより解読可能なコンピュータプログラムコード手段を実装したコンピュータで利用可能な媒体を有するコンピュータプログラム製品であって、該コンピュータプログラム手段が、コンピュータによって、アプリケーションプログラムを認証するようにする第一のコンピュータプログラムコード手段と、コンピュータによって、該第一のコンピュータプログラムコード手段により得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶するようにする第二のコンピュータプログラムコード手段と、コンピュータによって、前記アプリケーションプログラムからの著作物データへのアクセス要求を受け、前記第二のコンピュータプログラムコード手段により記憶されている前記アプリケーションプログラムの認証結果が前記第一のコンピュータプログラムコード手段による認証の成功を示す時に要求された著作物データへのアクセスを許可するようにする第三のコンピュータプログラムコード手段とを有することを特徴とするコンピュータプログラム製品を提供する。

【００４２】本発明では、著作権ラベルを正しく管理すること、つまり、著作権ラベルを除去・改ざんしたりしないほか、一次著作物の著作権ラベルを反映した著作権ラベルを二次著作物に付加する、ということを著作物を扱うアプリケーションプログラムが遵守するものとする。これは、著作物と著作物を扱うアプリケーションプログラムの作成者が同一ならば実現可能であるほか、作成者が同一でなくても、アプリケーションプログラムを管理機関に登録することにしてもよい。上記の条件を満たすアプリケーションプログラムを著作権遵守アプリケーションプログラムと呼ぶ。

【００４３】実行時には、アプリケーションプログラムが著作権遵守アプリケーションプログラムであるかどうかを認証する。例えば、ＯＳで管理されるファイルなどのデータには、そのデータが著作物であるかどうかを判断するための情報が付加される。

【００４４】著作権遵守アプリケーションプログラムであることが認証されたアプリケーションプログラムには、著作権データを直接読むことを許すほか、著作物データを作成する（データに著作権ラベルをつける）ことも許す。著作権遵守アプリケーションプログラム以外のアプリケーションプログラムには、著作物データを直接読み書きすることを許さない。

【００４５】さらに、本発明では、著作権遵守アプリケーションプログラムを実行させるプロセッサと、認証や認証結果を格納させるプロセッサとを、互いに異なるものとする。これによってさらに、認証や著作権データ管

理など著作物管理に関わらない前者のプロセッサに係わる部分の管理だけを利用者が行なえるようにし、一方、システム管理者の権限で著作権データ等を不正に管理するなどができないようにすることが可能となる。よって、極めて高いセキュリティを実現できる。また、本体のＯＳおよびアプリケーションプログラムへの侵入が生じた場合でも、別プロセッサに係わる認証結果が改ざんされにくいため、著作権の侵害をより効果的に防止することができる。

【００４６】このように本発明によれば、著作権ラベルの管理を正しく行なうアプリケーションプログラムのみが著作物を操作でき、それ以外のアプリケーションプログラムからの著作物の操作を禁止できるため、著作権の侵害の危険なしに計算機システム上で著作物を処理することができる。

【００４７】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態を説明する。

【００４８】（第１の実施の形態）本実施の形態は、概略的には、著作権カーネルと認証結果記憶機構をＯＳ内に設け、デジタル署名を用いてアプリケーションプログラムの認証を行なうものである。

【００４９】図１に、本実施の形態の概略的なシステム構成図を示す。本実施の形態では、アプリケーションプログラム６のベンダは、アプリケーションプログラム６が著作権ラベルを正しく管理することを保証するものとする。すなわち、アプリケーションプログラム６は、著作権ラベルを除去・改ざんしたりしないほか、一次著作物の著作権ラベルを反映した著作権ラベルを二次著作物に付加する、ということを著作物を扱うアプリケーションプログラムが遵守するものとする。これは、著作物と著作物を扱うアプリケーションプログラムの作成者が同一ならば実現可能であるほか、作成者が同一でなくても、アプリケーションプログラムを管理機関に登録することにしてもよい。上記の条件を満たすアプリケーションプログラムを、「著作権遵守アプリケーションプログラム」と呼ぶ。

【００５０】以下、本実施の形態の動作を図２のフローチャートと図３の動作説明図に基づいて説明する。まず、ＣＰＵ１上で実行されるオペレーティングシステム（ＯＳ）３内の著作権カーネル４は、アプリケーションプログラム６を認証し、アプリケーションプログラムが登録されたものであるかを判定する（図２のＳ５１，図３中のａ）。認証の結果、著作権ラベルを正しく管理するアプリケーションプログラムであることが判明した場合は、ＯＳ内にある認証結果記憶部５中にその旨を記憶しておく（図２のＳ５２，図３中のｂ）。

【００５１】その後、通常のアプリケーションの処理が行なわれ（図２のＳ５３）、アプリケーションプログラム６から著作物データの読み書き要求がＯＳに対して発

せられた際には（図２のＳ５４，図３中のｃ）、ＯＳ３は上記の認証結果記憶部５中を調べ（図２のＳ５５，図３中のｄ）、アプリケーションプログラム６が著作権ラベルを正しく管理するもの（著作権遵守アプリケーションプログラム）であることが確認されたときはその要求を認めるが（図２のＳ５６，図３中のｅ）、そうでなければ要求を拒否する。これによって、著作物管理を正しく行なうことができる。

【００５２】本システムは、外部と通信装置２（例えばモデム、ＬＡＮアダプタカード、ＳＣＳＩインタフェースカードなど）によって接続され、図示しないネットワーク経由にて外部との間で著作物データをやり取りすることができる。ネットワーク上の著作物データは、暗号化などの手段を利用することによって保護することが可能である。

【００５３】本実施の形態では、ＯＳ３の管理は、著作物管理を行なう組織の管理者が行ない、このシステムを利用する組織または個人（以下「利用者」）に対してシステム管理を行なう機能は提供しないものとする。このため、著作権カーネル４や認証結果記憶部５を改ざんすることはできないので、著作物は正しく管理される。

【００５４】さて、本実施の形態では認証の方法として、公開鍵暗号方式を用いたアプリケーションプログラムの実行ファイルへのデジタル署名を用いることができる。

【００５５】図４は、本実施の形態の認証を行なう部分の概略構成図である。アプリケーションプログラム６のベンダは、アプリケーションプログラム６が著作権ラベルを正しく管理することを確認した後、非公開の暗号化鍵を用いてアプリケーションプログラム６を暗号化する。利用者には、この暗号化されたファイルを配布する。アプリケーションプログラム６を復号化するための復号化鍵は、公開しておく。あるいは、復号化鍵は、アプリケーションの使用を許可されている使用者に対してのみあらかじめ渡しておくようにしても良い。

【００５６】ＯＳ３内には、著作権カーネル４と呼ばれる部分があり、ここで著作権に関連する処理を行なう。以下、著作権カーネル４での具体的な処理について述べる。

【００５７】アプリケーションプログラム６の実行時には、著作権カーネル４が、暗号化された（アプリケーションプログラム６Ａの）ファイルを公開鍵によって復号化する（図４中のａ）。復号が成功すれば、それはアプリケーションプログラム６が正しく認証されたことになるので、得られた平文の実行ファイル（アプリケーションプログラム６Ｂ）を実行するとともに、認証結果記憶部５に認証が成功した旨を記憶する（図４中のｂ）。

【００５８】図５は、図４の認証結果記憶部５内に設けられた管理テーブルの構造を示す図である。各アプリケーションプログラムごとに、そのアプリケーションプロ

グラムが著作権遵守アプリケーションプログラムであるかどうかが記憶されている。

【００５９】この実施の形態によれば、著作権遵守アプリケーションプログラムと、利用者が独自に作成したそれ以外のアプリケーションプログラムとを区別することができる。また、利用者が、著作権遵守アプリケーションプログラムをリバースエンジニアリングによって解析した上で改ざんして著作権ラベルを不正に操作するように改造しようとしても、著作権遵守アプリケーションプログラムが非公開鍵によって暗号化されているため、一般利用者には正しく暗号化を行なうことができず、復号化の際に正しく復号化されないことによって改ざんが発覚する。

【００６０】このように本実施の形態によれば、デジタル署名を用いた認証によって著作権遵守アプリケーションプログラムが判別でき、アプリケーションプログラムが著作権ラベルを不正に操作することによる著作権の侵害を防止できる。また、利用者がアプリケーションプログラムを解析して変更することはできないので、高いセキュリティを実現することができる。

【００６１】ここで、著作権の侵害の可能性については、認証されたアプリケーションプログラムは著作権ラベルの管理を正しく行なうことをアプリケーションプログラム作成者が保証しているため、これらのアプリケーションプログラムが著作権を侵害することはない。また、認証されていないアプリケーションプログラムが著作物データを読み書きすることを禁じることができるため、これらのアプリケーションプログラムによって著作権が侵害されることもない。

【００６２】著作権遵守アプリケーションプログラムのみが著作物を読んだり一次著作物からの二次著作物の作成を行ったりすることができるため、アプリケーションプログラムが渡された著作物データを自由に処理することができる。また、アプリケーションプログラムにデータを直接渡さないシステムと比べ、既存のアプリケーションプログラムにわずかな改造を加えるだけで著作権ラベルを正しく扱うアプリケーションプログラムにすることが可能である。またその際、著作物の処理を行う場合にＯＳを毎回呼び出す必要がないため、実行速度の向上を図ることができる。

【００６３】また、一次著作物の二次著作物での（二次利用）の細かい管理が可能になるという利点もある。一般に、一次著作物のどの部分がどの二次著作物に二次利用されているかという情報は、アプリケーションプログラムでの処理の詳細を把握していないＯＳで管理することは困難である。このような二次利用関係はアプリケーションプログラムがもっとも正確に把握している。

【００６４】本実施の形態では、アプリケーションプログラムが著作物データを生成することを許すため、アプリケーションプログラムが二次著作物の著作権ラベルを生成することができる。このため、一次著作物の著作権を二次著作物に正確に反映することができる。

【００６５】次に、上記第１の実施の形態に対する変形例１～変形例９を説明する。

（変形例１）認証の方法として、第１の実施の形態のデジタル署名の代わりにパスワードを用いることができる。

【００６６】図６は、変形例１の認証を行なう部分の概略構成図である。この他の部分は第１の実施の形態（図１）と同様であるので省略する。

【００６７】本変形例１では、アプリケーションプログラム６はパスワードを持っており、アプリケーションプログラム６の実行時にＯＳ３に対して自分が持っているパスワードを提示する（図６中のａ）。著作権カーネル４はアプリケーションプログラム６のＩＤとパスワードをパスワード記憶部１５中に格納された各著作権遵守アプリケーションプログラムのＩＤおよび全ての著作権遵守アプリケーションプログラムに共通なパスワードと照合し（図６中のｂ）、正しいパスワードが提示された場合にのみ、認証結果記憶部５に認証が成功した旨を記憶する（図６中のｃ）。

【００６８】本変形例１は、暗号化が不要であることから、第１の実施の形態に比較して、アプリケーションプログラムの起動がより高速であるとともに、装置構成が簡略化されるという利点がある。

【００６９】（変形例２）図７は、変形例２の認証を行なう部分の概略構成図である。この他の部分は第１の実施の形態（図１）と同様であるので省略する。

【００７０】変形例１では、パスワードが固定されていると、そのパスワードが漏洩した場合に認証が正しく行なわれない場合がある。この変形例２では、全ての著作権遵守アプリケーションプログラムに共通なパスワードを一つではなく複数用意しておく。具体的には、合言葉を取り決めておき、ＯＳ３側がまず取り決めておいた単語（数値などを含む）を一つ選んでアプリケーションプログラム６に通知する（図７中のａ）。アプリケーションプログラム６は、その合言葉に対してあらかじめ決められた返答を返す（図７中のｂ）。著作権カーネル４は、その返答をパスワード記憶部１５内の返答と照合し（図７中のｃ）、正しい返答を答えた場合のみ、認証結果記憶部５に認証が成功した旨を記憶する（図７中のｄ）。

【００７１】本変形例２は、パスワードの漏洩によってアプリケーションプログラム６が正しく認証できなくなる危険が変形例１より小さい利点がある。

【００７２】（変形例３）本変形例３は、システムから著作物管理を行なう部分とそうでない部分を互いに分離し、それらを異なるハードウェア上で実現することによって、著作物管理に関わらない部分の管理だけを利用者が行なえるようにし、一方、システム管理者の権限で著

作権ラベルを不正に管理することができないようにして、極めて高いセキュリティを実現できるようにしたものである。これによって、ＵＮＩＸなどの従来のＯＳをベースにしてシステムを構成することができる。

【００７３】図８に、本変形例の概略的なシステム構成図を示す。著作物管理を行なう著作権カーネル４と認証結果記憶部５とを本体ＯＳ１４から分離し、それらを別のＣＰＵ２１上に搭載し、本体ハードウェア３０のＣＰＵ１１と別ハードウェア３２の別ＣＰＵ２１との間をバス１２によって結合する。

【００７４】本変形例３の処理の手順は、第１の実施の形態と同様である。まず、アプリケーションプログラム６のベンダは、アプリケーションプログラム６が著作権ラベルを正しく管理することを保証するものとする。このような保証が行なわれたアプリケーションプログラム６は、あらかじめ著作物管理を行なう組織に登録される。

【００７５】別ＣＰＵ２１上にて提供される著作権カーネル４は、アプリケーションプログラム６を認証し、アプリケーションプログラムが登録されたものであるかを判定する（図８中のａ）。認証の結果、著作権ラベルを正しく管理するアプリケーションプログラムであることが判明した場合は、認証結果記憶部５中にその旨を記憶しておく（図８中のｂ）。

【００７６】その後、アプリケーションプログラム６から著作物データの読み書き要求が本体ＯＳ１４に対して発せられた際には（図８中のｃ）、本体ＯＳ１４は上記の認証結果記憶部５中を調べ（図８中のｄ）、アプリケーションプログラム６が著作権ラベルを正しく管理するもの（著作権遵守アプリケーションプログラム）であることが確認されたときはその要求を認めるが（図８中のｅ）、そうでなければ要求を拒否する。

【００７７】これによって、悪意の管理者が本体ハードウェア３０側の本体ＯＳ１４の設定を書き換えて著作物データを改ざんしようとしても、著作物データを管理する著作権カーネル４および認証結果記憶部５はハードウェア的に分離されているため、改ざんすることはできない。したがって、本体ハードウェア３０を利用者に管理させても著作物を正しく管理することができる。

【００７８】（変形例４）アプリケーションプログラム６の認証が正しく行なわれても、本体ＯＳ１４が改ざんされると、著作物の読み書き可否判定を正しく行なわないようにしたり、著作物データを正しく管理できないようにされたりする危険がある。

【００７９】これを防ぐため、変形例３を修正し、計算機システムの起動時に本体ＯＳ１４の認証を行なうようにしたのが本変形例である。

【００８０】本変形例４の概略構成図を、図９に示す。計算機システムの起動時には、まず別ＣＰＵ２１が起動され（図９中のａ）、その後に本体ＣＰＵ１１上の本体ＯＳ１４が起動する際（図９中のｃ）に、別ＣＰＵ２１上のプログラムによって本体ＣＰＵ１１上の本体ＯＳ１４が認証される（図９中のｂ）。

【００８１】別ＣＰＵ２１による本体ハードウェア３０側の本体ＯＳ１４の認証方法としては、前述したＯＳによるアプリケーションプログラムの認証と同様の方法が利用できる。

【００８２】（変形例５）第１の実施の形態では、各アプリケーションプログラムで個別に著作権ラベルの読み書きをする。この操作を一つのプログラムにまとめたものを著作権ラベル読み書きプログラムとし、このプログラムを著作権遵守アプリケーションプログラムが呼び出して、著作権ラベルの読み書きをさせるようにすることもできる。

【００８３】本変形例５の概略構成図を、図１０に示す。各アプリケーションプログラム６１～６３夫々は、著作権ラベル読み書きプログラム６４を呼び出し（図１０中のａ）、呼び出された著作権ラベル読み書きプログラム６４が、実際の著作権ラベル１６０の読み書きを行なう（図１０中のｂ）。

【００８４】この変形例によると、アプリケーションプログラムごとに著作権ラベルの読み書き処理を行なうルーチンを作らずに済み、開発効率が上がるほか、アプリケーションプログラムがライブラリ、即ち著作権ラベル読み書きプログラム、を正しく利用するかぎり、著作権ラベルに対して誤った管理が行なわれる可能性がなくなる。

【００８５】（変形例６）第１の実施の形態においては、認証されていないアプリケーションプログラムについては、著作物データの読み書き両方を禁止していたが、本変形例６は、書き込みのみを禁止し、読み出しは認証されていないアプリケーションプログラムについても許す。

【００８６】このようにしても、アプリケーションプログラムが著作物を他へコピーすることができないので、著作権侵害を防止するという目的を達成することができる。

【００８７】（変形例７）第１の実施の形態では、アプリケーションプログラムは著作権遵守アプリケーションプログラムであるかそうでないかの二通りに分類し、唯一の機関がアプリケーションプログラムの管理を行い、著作物を操作するすべてのアプリケーションプログラムはその機関に登録するものであった。

【００８８】本変形例では、上記の分類を細分化し、「各著作物のベンダがどのアプリケーションプログラムを信頼するか」を自由に決定することができるようにする。これによって、集中管理を行なう管理機関が不要となる利点がある。

【００８９】また、各著作物を作成するベンダが、信頼できるベンダ、つまり自社・関連会社・契約を行なった

会社などが作成したアプリケーションプログラムからの読み書きのみを個別に許すことができるため、著作権の保護をよりきめ細かく行なうことができる。

【００９０】図１１が、本変形例における認証結果記憶部５内に設けられた管理テーブルの構造を示す図である。各アプリケーションプログラムごとに、そのアプリケーションプログラムがどの著作物を読み書きすることが許されているか、が記憶されている。即ち、各アプリケーションプログラムが各著作物について認証されたかどうかが記憶されている。

【００９１】本変形例では、認証として、第１の実施の形態または変形例１，２と同じ方法を用いれば良い。

【００９２】本変形例によれば、万一著作物ラベルを正しく管理しないアプリケーションプログラムが登録されても、広い範囲で著作権侵害が生じることを防止することができる。

【００９３】（変形例８）第一の実施の形態では、認証を予め行っているが、これを変形して、アプリケーションプログラムが著作物の読み書き要求を行ったときにはじめて認証を行うようにすることも可能である。この場合、システム構成は上述した図１に示すものと同様である。

【００９４】以下、図１２に示すフローチャートに従って、本変形例における動作手順を説明する。

【００９５】まず、ＣＰＵ１上で実行されるアプリケーションプログラム６の通常の処理が行われ（図１２のＳ６１）、アプリケーションプログラム６からＯＳ３に対して著作物の読み書き要求が発せられた場合（図１２のＳ６２）、ＯＳ３は内部の認証結果記憶部５を調べて、アプリケーションプログラム６の認証が既に行われているかどうか確かめる（図１２のＳ６３）。

【００９６】まだ認証が行われておらず、認証結果記憶部５にアプリケーションプログラム６の認証結果が記録されていない場合には、ＯＳ３内の著作権カーネル４がアプリケーションプログラム６を認証し、このアプリケーションプログラムが登録されたものであるかどうか判定する（図１２のＳ６４）。この認証の結果、著作権ラベルを正しく管理するもの（著作権遵守アプリケーションプログラム）であるかが判明し、その認証結果を認証結果記憶部５中に記憶しておく。

【００９７】次に、ＯＳ３は上記の認証結果記憶部５を調べて、このアプリケーションプログラム６が著作権ラベルを正しく管理するもの（著作権遵守アプリケーションプログラム）であるときにはその要求を認め、そうでないときにはその要求を拒絶する（図１２のＳ６６）。これによって、著作物管理を正しく行うことができる。

【００９８】本変形例では、アプリケーションプログラムの起動時に認証が行われないために起動速度が向上するほか、著作物を読み書きしないアプリケーションプログラムについては認証処理が全く行われないために上記第一の実施の形態に比べて実行速度が向上するというメリットがある。

【００９９】（変形例９）この変形例９は、上述した第一の実施の形態を、本発明者による特願平６－２２１２３５に開示されたデータ入出力管理装置と組合せることにより、著作物データの入出力を管理するようにしたものである。

【０１００】この場合のシステム構成を図１３に示す。図１３において、著作権カーネル４と認証結果記憶部５は上述した第一の実施の形態におけるものと同様の機能を有するものであり、これらを含んだデータ入出力管理装置１００が著作物データの読み書き（入出力）を要求する入出力要求プログラム１１１に対して提供されている。図１３のシステムにおけるデータ入出力管理装置１００は更に入出力要求受理部１０１，データ入力部１０２，保護データ判定部１０３，保護データ入力記憶部１０４，出力許諾判定部１０５，データ出力部１０６を含む。このデータ入出力管理装置１００全体はプロセッサ上のＯＳで実現できる。

【０１０１】図１３のシステムにおいて、入出力要求プログラム１１１からの著作物データの読み書き（入出力）要求は、著作権カーネル４と認証結果記憶部５の動作により上述した第一の実施の形態同様このプログラムが著作権ラベルを正しく管理するもの（著作権遵守アプリケーションプログラム）であるとき許可されるほか、著作権遵守アプリケーションプログラムでないプログラムについても著作物データが複製される恐れのない場合には著作物のデータの入出力を認めるようにデータの入出力管理が行われる。

【０１０２】このようにしても、著作権遵守アプリケーションプログラムでないプログラムが著作物データをコピーすることは出来ないので、著作権侵害を防止するという目的を達成することができる。

【０１０３】ここで、図１３のシステムにおける著作物データの入出力要求に対する動作を簡単に説明するが、詳細は特願平６－２２１２３５にあるので省略する。

【０１０４】まず入出力要求プログラム１１１が要求を発生すると、入出力要求受理部１０１がこの要求を受理し、入出力要求プログラム１１１の識別子と要求の種類を判別する。

【０１０５】これにより入力要求であることが分ると、データ入力部１０２が要求されているデータを記憶媒体やネットワーク等から入力する。この時、保護データ判別部１０３が入力を要求されたデータが保護データ（出力について所定の保護が与えられることを要求されているデータで著作物データを含むもの）であるか否かを判別する。この判別の結果、保護データを含むものであった場合は、保護データ入力記録部１０４にこの保護データの入力を要求したプログラムの識別子を記録する。そして、入出力要求プログラム１１１に要求されたデータ

を与える。

【０１０６】一方、出力要求であった場合には、著作権遵守アプリケーションプログラムかどうかで処理が異なる。著作権カーネル４に問い合わせを行うことによって認証結果記憶部５を調べ、著作権遵守アプリケーションプログラムであると分った場合には出力を許可する。一方、そうでない場合には、以下の処理を行う。

【０１０７】出力許諾判定部１０５が保護データ入力記録部１０４を調べてこの出力要求を発したプログラムの識別子が記録されているかどうか、即ち、このプログラムが保護データを読んだものであるかどうか、を判定する。ここでこのプログラムの識別子が保護データ入力記録部１０４に記録されていなければ、このプログラムは保護データを持っていないことになり、このプログラムからの出力要求により保護データが出力される可能性はないので、この場合には出力要求を許諾する。

【０１０８】これに対し、このプログラムの識別子が保護データ入力記録部１０４に記録されていれば、このプログラムは保護データを持っていることになり、このプログラムからの出力要求により保護データが出力される可能性がある。従って、この場合には、要求されている出力先に応じて出力要求を認めるかどうか出力許諾判定部１０５が判断する。ここで、要求されている出力先がディスプレイのように他のプログラムがそこから直接データを読み込めない出力機器である場合には出力要求を許諾し、そうでなければ保護データが複製される恐れがあるため出力要求を拒絶する。出力要求が許諾される場合には、データ出力部１０６から要求されたデータの出力が行われる。

【０１０９】これにより、保護データを読んだことのないプログラムからは自由にデータの入出力が行え、且つ、保護データを読んだプログラムからの出力は保護データが複製される恐れのない場合にのみ許可するようにデータ入出力管理が行える。

【０１１０】なお、本発明は上述した各実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で、種々変形して実施することができる。

【０１１１】尚、当業者に明らかなように、上述した本発明の実施の形態及びその変形例は、一般の汎用コンピュータを適当にプログラムすることでも実現可能である。この場合に必要となるソフトウェアコードは上述した記載から当業者レベルのプログラマーによって容易に作成可能である。

【０１１２】特に、上記実施の形態における著作権カーネル４と認証結果記憶部５の機能をソフトウェアパッケージとして実装すると効果的である。

【０１１３】そのようなソフトウェアパッケージは、上述したような本発明の機能、動作をコンピュータに実現させるようにプログラムするためのコンピュータコードを格納する記憶媒体を用いたコンピュータプログラム製品の形で提供可能であり、この際の記憶媒体としては、従来のフロッピーディスク、オプティカルディスク、ＣＤ－ＲＯＭ、磁気光学ディスク、ＲＯＭ、ＲＡＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、磁気又は光学カード等を含む電子的な命令の格納に適したあらゆる種類の記憶媒体を使用し得るものである。

【０１１４】

【発明の効果】以上説明したように本発明によれば、アプリケーションプログラムを認証し、その結果を記録するとともに、あるアプリケーションプログラムから著作物データへのアクセス要求があった場合、該アプリケーションプログラムが認証済であるときに限り該アクセス要求を許可するようにしたので、著作権ラベルの管理を正しく行なうものとして登録されたアプリケーションプログラムのみが著作物を操作でき、それ以外のアプリケーションプログラムからの著作物の操作を禁止できるため、著作権の侵害の危険なしに計算機システム上で絵画・小説などの受動的なデータである著作物を処理することができる。

【０１１５】さらに、本発明では、著作権遵守アプリケーションプログラムを実行させるプロセッサと、認証や認証結果を格納させるプロセッサとを、互いに異なるものとすることによって、認証や著作権データ管理など著作物管理に関わらない前者のプロセッサに係わる部分の管理だけを利用者が行なえるようにし、極めて高いセキュリティを実現できる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態の全体の構成を示すブロック図。

【図２】図１の構成における動作を示すフローチャート。

【図３】図１の構成における動作を説明するための図。

【図４】図１の構成においてアプリケーションプログラムの認証を行なう部分の構成を示す図。

【図５】図１の構成における認証結果記憶部の内部構造を示す図。

【図６】変形例１においてアプリケーションプログラムの認証を行なう部分の構成を示す図。

【図７】変形例２においてアプリケーションプログラムの認証を行なう部分の構成を示す図。

【図８】変形例３の構成を示すブロック図。

【図９】変形例４においてＯＳの認証を行なう部分の構成を示す図。

【図１０】変形例５において著作権ラベルの読み書きを行なう部分の構成を示す図。

【図１１】変形例７における認証結果記憶部の内部構造を示す図。

【図１２】変形例８における動作を示すフローチャート。

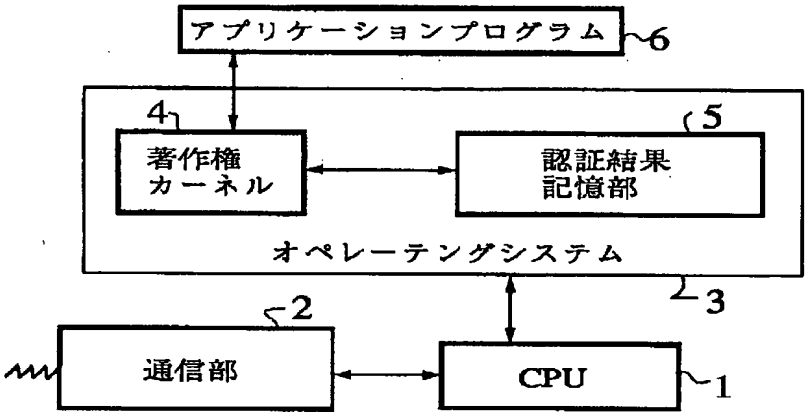
【図１３】変形例９の構成を示すブロック図。

21　　22

【符号の説明】

1　マイクロプロセッサ（ＣＰＵ）
2　通信部
3　オペレーティングシステム（ＯＳ）
＊4　著作権カーネル
5　認証結果記憶部
6　アプリケーションプログラム
＊

【図１】



【図２】　Fig. 2

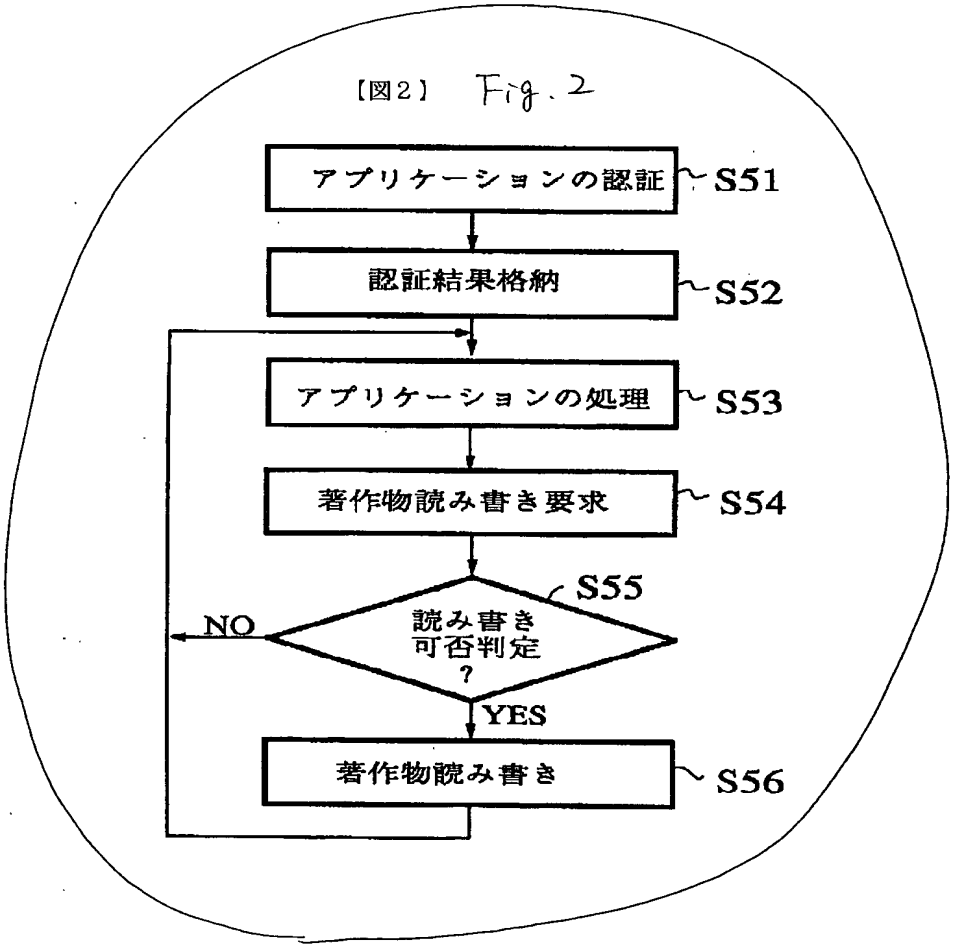
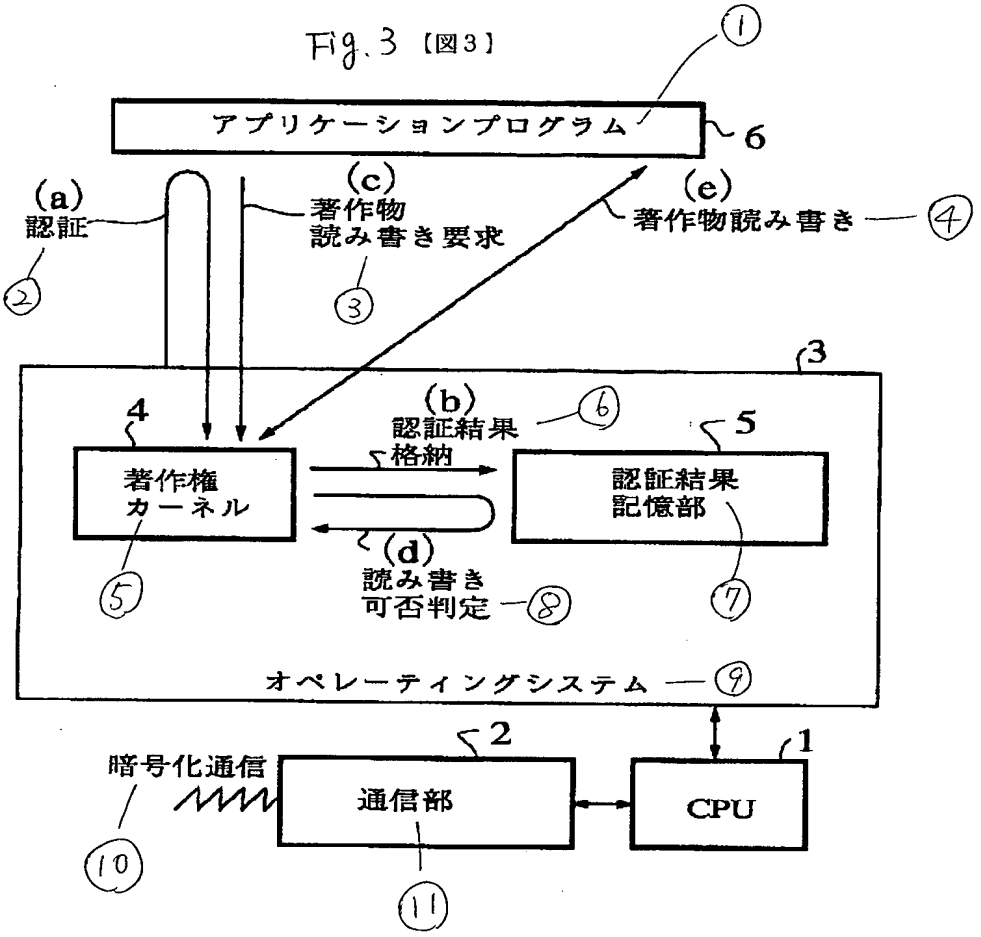
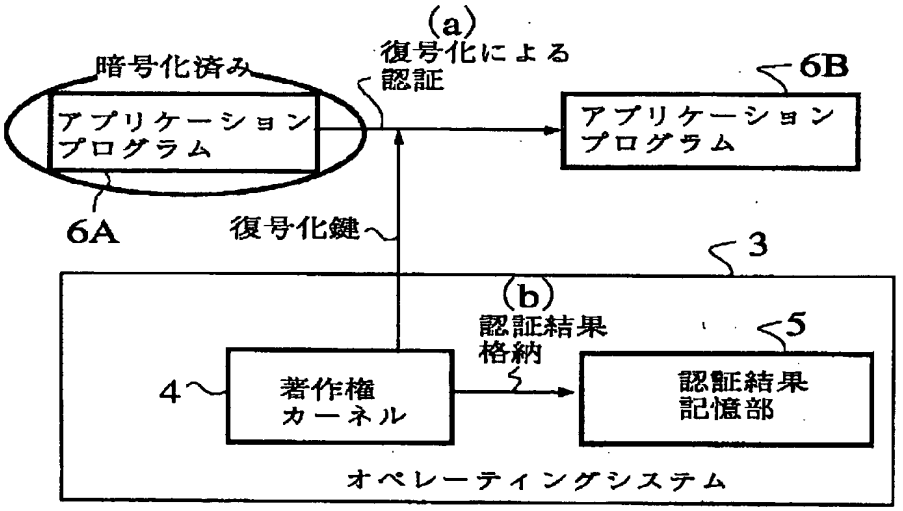


Fig. 3 【図3】


①
アプリケーションプログラム
6
(a)
認証
②
(c)
著作物
読み書き要求
③
(e)
著作物読み書き
④
3
4
(b)
認証結果
格納
⑥
5
著作権
カーネル
⑤
(d)
読み書き
可否判定
⑧
認証結果
記憶部
⑦
オペレーティングシステム
⑨
2
1
暗号化通信
⑩
通信部
CPU
⑪

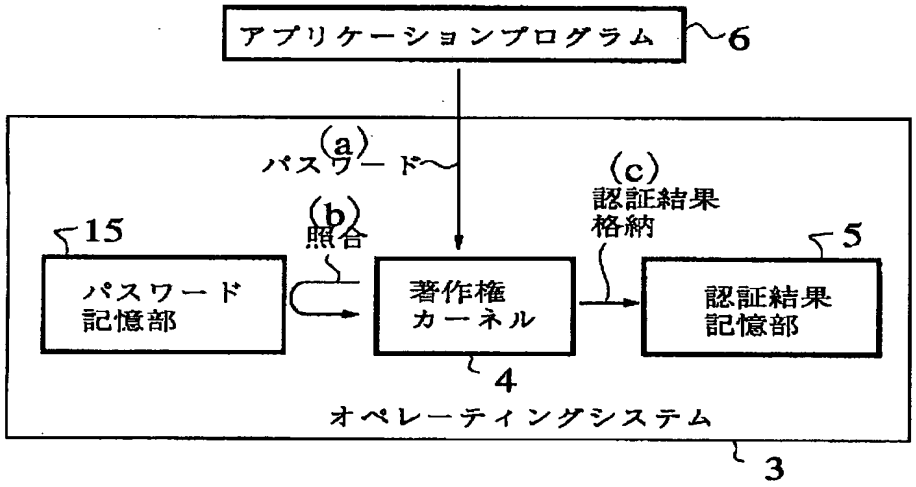
【図4】


(a)
復号化による
認証
暗号化済み
アプリケーション
プログラム
6A
6B
アプリケーション
プログラム
復号化鍵
3
(b)
認証結果
格納
5
4
著作権
カーネル
認証結果
記憶部
オペレーティングシステム

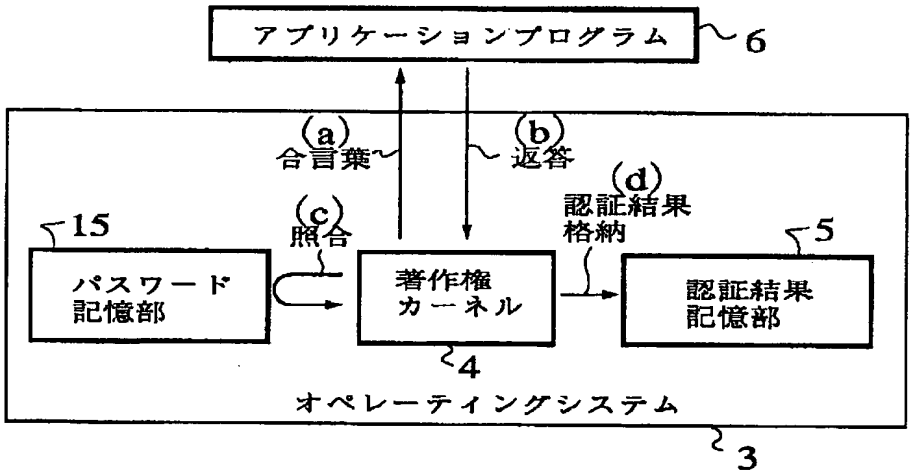
【図５】

	認証結果
アプリケーション プログラム 1	○
アプリケーション プログラム 2	×
.....	.....
アプリケーション プログラム n	○

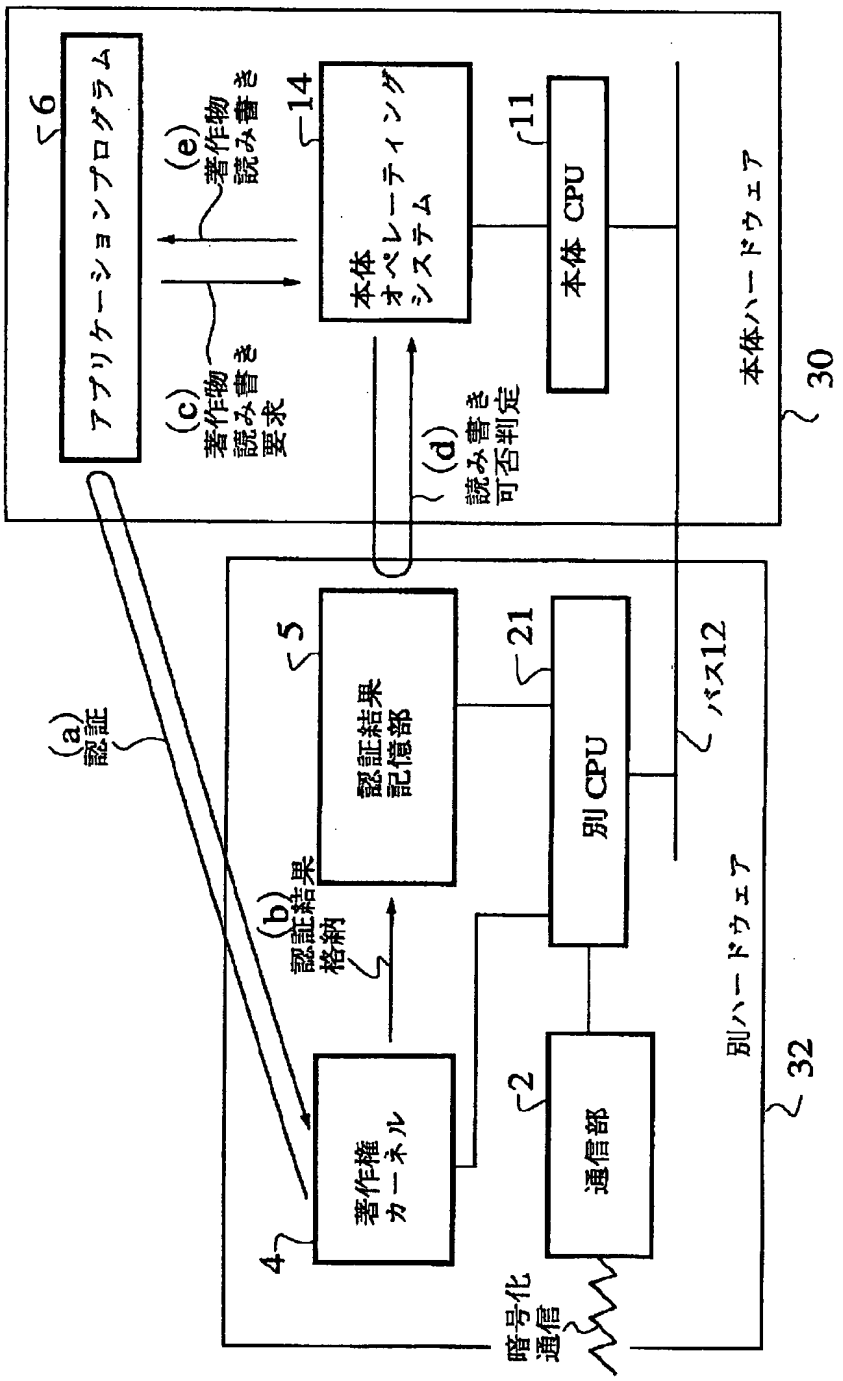
【図６】



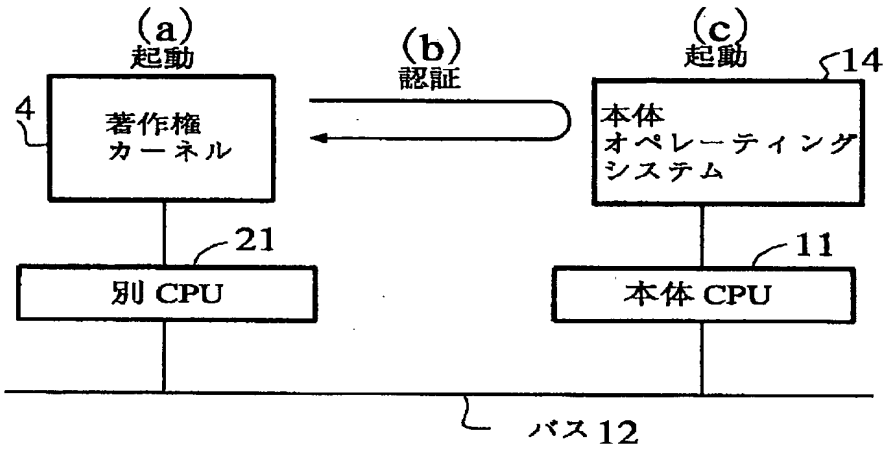
【図７】



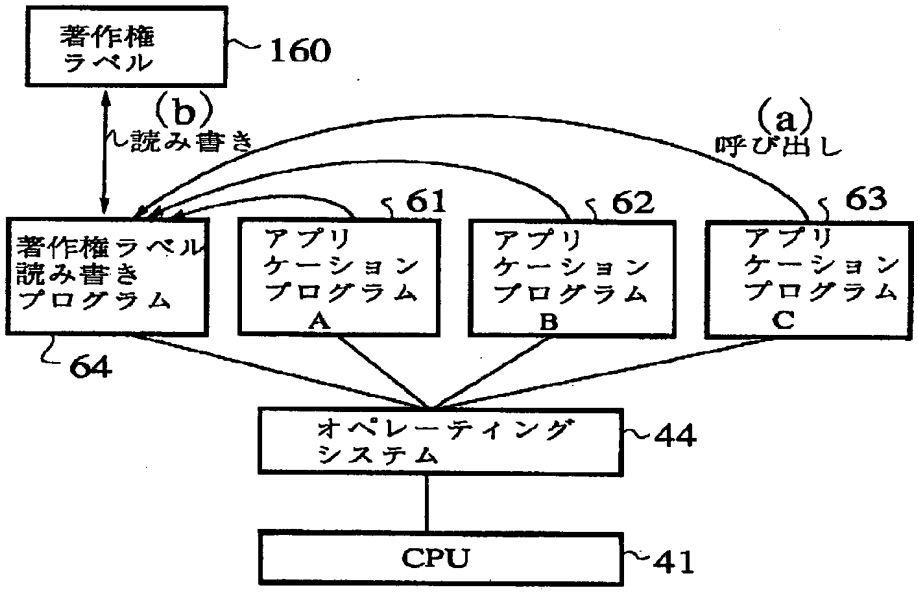
【図8】


アプリケーションプログラム
6
(e)
著作物
読み書き
14
本体
オペレーティング
システム
11
本体 CPU
本体ハードウェア
30
(c)
著作物
読み書き
要求
(d)
読み書き
可否判定
(a)
認証
5
認証結果
記憶部
21
別 CPU
バス12
(b)
認証結果
格納
著作権
カーネル
4
2
通信部
別ハードウェア
32
暗号化
通信

【図９】



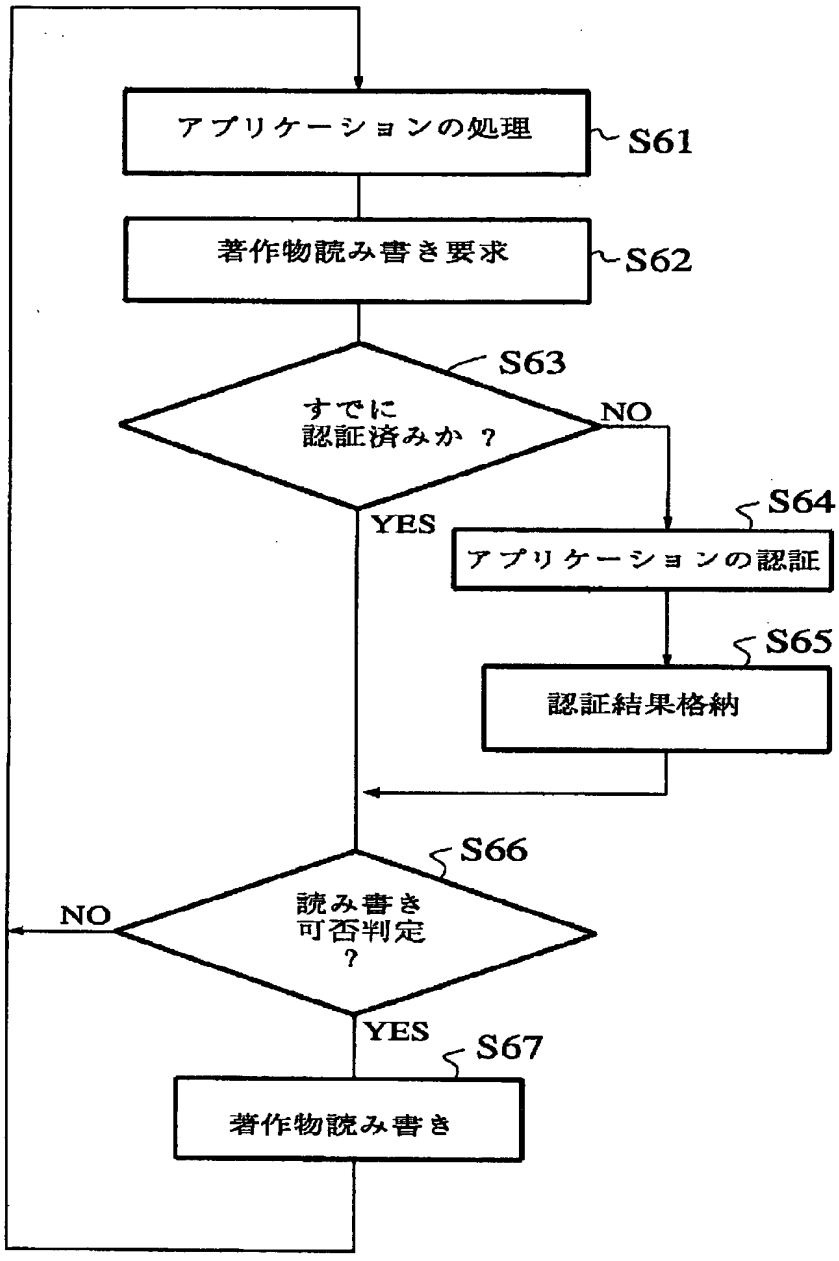
【図１０】



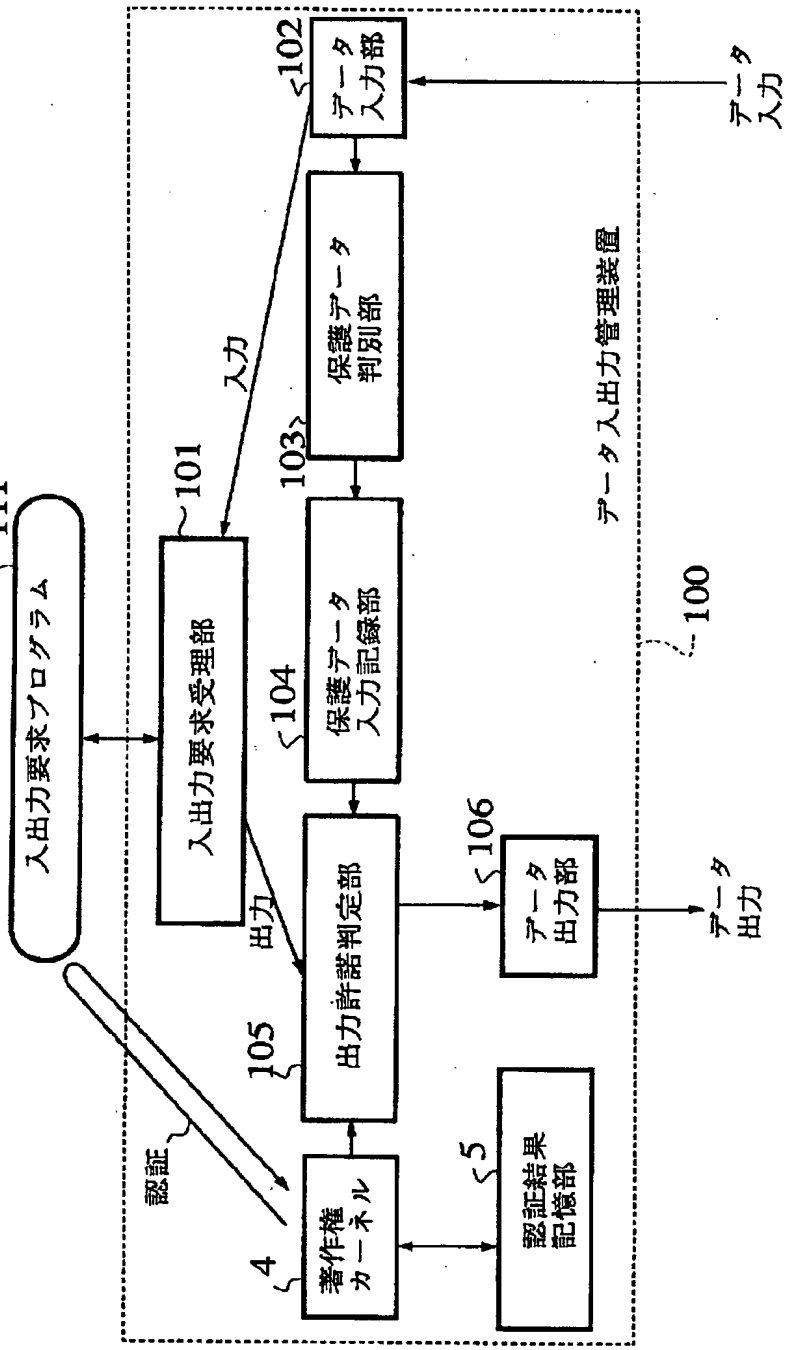
【図１１】

	著作物１	著作物２	……	著作物ｎ
アプリケーション プログラム１	○	○	……	×
アプリケーション プログラム２	×	○	……	○
……	……	……	……	……
アプリケーション プログラムｎ	○	×	……	×

【図１２】


アプリケーションの処理
S61
著作物読み書き要求
S62
S63
すでに
認証済みか ？
NO
YES
S64
アプリケーションの認証
S65
認証結果格納
S66
読み書き
可否判定
？
NO
YES
S67
著作物読み書き

【図１３】


データ入出力管理装置
100
入出力要求プログラム
111
入出力要求受理部
101
データ入力部
102
保護データ判別部
103
保護データ入力記録部
104
出力許諾判定部
105
データ出力部
106
著作権カーネル
4
認証結果記憶部
5
入力
出力
認証
データ入力
データ出力